American Financial Services Association
919 Eighteenth Street, NW • Washington, DC • 20006
phone 202 296 5544 • fax 202 223 0321 • email afsa@afsamail.org
www.afsaonline.org

The Market Funded Lending Industry

January 19, 2007

Federal Trade Commission/
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, DC 20850

RE: Identity Theft Task Force, P065410

Dear Sir or Madam:

The American Financial Services Association thanks you for the leadership role you have taken to protect consumers from identity theft and fraud. We appreciate the opportunity to comment on the President's Identity Theft Task Force and the interim recommendations put forth in September, 2006.

The American Financial Services Association (AFSA) is the trade association for a wide variety of non-traditional, market-funded providers of financial services to consumers and small businesses. Founded in 1916, AFSA represents approximately 360 non-traditional market-funded providers of financial services to consumers and small businesses. As adopted by our members, the mission of AFSA "is to assure a strong and healthy broad-based consumer lending services industry which is committed to: (1) providing the public with quality and cost effective service, (2) promoting a financial system that enhances competitiveness and (3) supporting the responsible delivery and use of credit and credit related products."

AFSA recognizes that the issue of identity theft is crucially important to President Bush and his Administration. We believe that an effective coordination between government and private sector in the areas of criminal prosecution of identity thieves, data safeguarding, public awareness and guidance, and improved loss recovery will help protect both consumers and businesses from this very real threat.

To that end, we would like to offer our input on some of the questions posed in the Task Force's notice for public comments. In addition, we would like to offer some general observations on issues that we feel should be highlighted or addressed by the Task Force, but are not evident from the questions.

Maintaining Security of Consumer Data - Government and Private Sector Use of Social Security Numbers

AFSA believes that Social Security Numbers ("SSNs") are the most effective, and only universal and consistent, data element used to authenticate a person's identity. The need for SSNs by the government for the purpose of Social Security benefits, law enforcement and identity verification, among other reasons, cannot be underscored.

Any discussion of a prohibition of government use of SSNs must take into consideration the overwhelming costs of such a conversion and the lack of progress this would actually net toward the real end of curbing identity theft. Any "alternative" unique identifier to SSNs will simply offer identity thieves a new target to acquire, rather than resolve the current concerns about SSN use for ID theft purposes. In addressing the issue of *stolen data*, it is reasonable to surmise that if would-be thieves are sophisticated enough in their methods to acquire SSNs from the government, they will be sophisticated enough to acquire any alternative identifier for their use as well.

However when focusing on *lost data*, AFSA does believe that the prohibition of display of SSNs on government forms or records that are publicly available – drivers licenses, state ID cards, tax forms, government checks or deeds – would lessen the risk of identity theft simply by these documents falling into the wrong hands.

Similar to the government use of SSNs, the SSN is the only consistent and universally accepted form of identification used in commerce for purposes of verification, fraud prevention and recovery, consumer credit applications, employment security and screening and "business-to-business" transactions. While names, addresses and phone numbers change millions of times a year, as well as the sharing of common names, SSNs are integral to authenticating whether an individual is who they claim to be for the purposes of a variety of commercial transactions. Therefore, restricting the use of SSNs would actually weaken the private sector's ability to prevent fraud and identity theft.

We do believe that, much like our recommendations on government use of SSNs, that reasonable restrictions on the display and public availability of SSNs by the private sector could be supported by our industry and readily implemented. Such restrictions could cover SSNs being required for online passwords or log-in information, and display on the internet, employee badges, health insurance cards or other means of identification that may be visible to other individuals.

We would urge the Task Force that any study concerning SSNs in the public and private sector, possible alternative identifiers and prohibitions on use, would include an evaluation of *benefits to consumers* that the responsible and legitimate use of SSNs brings. We would also ask the Task Force to consider the societal costs on government, industry and consumers of replacing SSNs with any alternative. And finally, we ask the Task Force to consider whether any alternative unique identifier would really achieve the

end goal of preventing identity theft. Rather would it simply give thieves another piece of data to steal, thus making the restoring of victims' credit files that much more difficult?

National Data Security Standards

AFSA recommends to the Task Force that any national data security standards should be based generally on the principles adopted in the Gramm-Leach-Bliley Act (GLBA) and the Federal Trade Commissions (FTC) "Safeguards Rule", where appropriate jurisdictions apply. Financial Institutions are already required to safeguard customer information, have a response program in the event sensitive customer information is compromised, and to provide notification to customers if warranted. The FTC Safeguards Rule imposes similar requirements on non-financial entities within its jurisdiction. In addition, financial institutions are required to comply with the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("Interagency Guidance") developed by the federal financial services regulators.

We ask that the Task Force not add duplicative, and potentially burdensome, new requirements to companies already covered by the above mentioned government regulations. Rather, we recommend that the efforts be on ensuring a national and uniform application of data security and breach notification standards to companies not currently covered by the existing regulatory regime. Such "safe harbor" provisions were in each of the five principal data security bills reported out of committee in the 109th Congress, and deemed companies in compliance with their current regulatory requirements to be covered in any national data security standard.

Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information

AFSA strongly supports the establishment of a uniform national standard for notification of a data breach that is reasonably likely to result in harm or inconvenience to the consumer. It is very important that the trigger for notification be risk-based to avoid broad over-notification of consumers that are not as risk of harm.

A federally-defined and enforced notification trigger that provides discretion to businesses to evaluate the facts and circumstances of a security breach to determine the potential risk to affected customers is a principle that AFSA supports, and one that the FTC and numerous proposed federal bills has endorsed. A threshold requirement, one based on a *"reasonable likelihood of misuse"*, would ensure that consumers are notified when actually are at risk of harm, and not unduly notified when there is little likelihood at all of harm or inconvenience. Over-notification of consumers would alarm them for no justifiable reason, and eventually desensitize them to notification when a true risk exists.

Preventing the Misuse of Consumer Data

Fully recognizing the threat posed by identity thieves and the importance of aggressive efforts to combat the changing nature of the crime, individual business and corporate leaders have often joined together in cross-industry initiatives aimed at reducing identity theft.

AFSA member companies have partaken in that effort by forming an Identity Theft Fraud Control Committee to serve as a conduit for member companies to join forces to deter, detect and prevent fraud based on ID theft. The committee will share best practices concerning security standards and data safeguarding; exchange information about proactive detection and investigation techniques; create an early warning system for new fraud threats emerging in the US; and develop consumer and industry fraud awareness initiatives. This is just one of the many proactive steps industry has taken to reduce the economic harm to both consumers and businesses resulting from theft or misuse of consumer data.

We ask that the Task Force recognize these efforts by industry to present a clear view to the President and to Congress when presenting its recommendations.

Victim Recovery

AFSA endorses the principles of restitution for victims of identity theft from the perpetrator of the crime. We do urge the Task Force to keep in mind that there are usually multiple victims to fraud and identity theft crimes. The companies and entities from which the personal data is stolen are also victims of a crime, even when no consumers are actually endangered or harmed as a result of it. Damaged corporate reputation and lost customer trust can have a major financial impact on companies, although it is often hard to quantify precisely. We ask that the Task Force strongly consider this when recommending its principles for restitution.

AFSA also supports a thorough assessment of existing remedies before determining the advisability of a "credit freeze" as a recovery measure for identity theft victims. The enactment of the FACT Act in 2003 created significant methods of identity theft prevention and mitigation. The Bush Administration was instrumental in ensuring that effective and robust consumer protections were included in the legislation. We have been surprised at the lack of attention to these improvements in the law and we urge the Task Force to consider the effectiveness of these and other identity theft victim mitigation measures before determining the need for additional laws.

Given the strong protections under the FACT Act, we feel that a credit freeze, in most circumstances, is an excessive step for consumers to take. A credit freeze can impose severe repercussions – such as impediments to instant credit and emergency credit, delays in locking a mortgage, and logistics involved in "thawing" their file - that may result in more harm than good to many consumers. Although we are confident that the Task Force

would consider the obvious costs associated with credit freeze laws, we also believe the Task Force should consider the broader impact freeze laws would have on the nationwide credit granting system the Bush Administration and vast majority of legislators touted as part of the enactment of the FACT Act. The Task Force should not only review the purported effectiveness of freeze laws and their costs, but also the significant detriments to consumers and the credit market in America.

If the Task Force determines that there are circumstances in which consumes should have the option to exercise a credit freeze as a "nuclear option," we ask that they convey the importance of using it as a last line of defense, rather than the first prevention technique employed.

Measuring Law Enforcement Efforts

While the task force has proposed a number of surveys and studies to conduct, AFSA recommends it recommend further study on the following questions:

- **Measurable Correlation Between Breaches and Instances of True Identity Theft.** The Task Force should recommend a study to determine the extent to which breaches of data security have actually resulted in instances of identity theft (defined as establishment of new accounts by fraudulent means through the misuse of personal information of individuals obtained as a result of the security breach.)

- **Sources of Personal Data Used By Identity Thieves, Including Legally Available.** The Task Force should recommend a study to determine the extent to which the source of personal information used by identity thieves (where known) was obtained through one of the following means:

    - Data security breach involving criminal intent of the perpetrators (e.g., theft of a laptop, computer hacking, stolen packages with backup takes, etc.);

    - Data security breach occurring as a result of business negligence or mishandling of data, including poor data security practices resulting in the unintentional making of confidential personal data publicly available;

    - Illegal purchases of SSNs via unfair or deceptive acts or practices;

    - Legal reviews of public records made available by governmental entities; and

    - Offline methods of gathering such information (e.g., "dumpster diving").

- **Prevalence of Over-Notification and Insufficiently High Notification Triggers.** The Task Force should recommend a study to determine the extent to

which those individuals who have been notified in 2005 and 2006 of data security breaches potentially affecting their personal information have actually become the victim of identity theft or suffered any other measurable harm.

In addition to our comments on these questions, we would like to stress the importance of two underlying principles we ask the Task Force to consider when crafting its recommendations. The accuracy of the definition in regards to *"personally identifiable information"* and *"identity theft"* is of paramount importance to the effectiveness of the Task Force's efforts.

Definitions for these terms have been hammered out in 35 state data breach bills already passed, and the 5 federal bills that were reported out of Committees last Congress. We ask the Task Force to recognize the work that has been done and build on it in its recommendations.

In defining "identity theft", AFSA believes the term should clearly include the type of fraud that occurs when an individual's personal information is used, without authorization, as false identification for the purposes of opening new financial accounts in that individual's name in order to defraud the individual and the business in which the account is opened. However, it is important that the term "identity theft" not include what industry would refer to as "credit card account fraud," or the type of fraud perpetrated by using an existing credit card number to make purchases of goods or services. These latter cases of credit card fraud have been addressed by criminal statute, law enforcement at all levels of government, and industry efforts for many years. In fact, credit card issuing banks and credit card networks bear nearly the entire cost of such fraud.

We have been encouraged by FTC Chairman Majoras's statements differentiating identity theft from other forms of fraud, such as credit card fraud. The tracking of consumer complaints by the FTC has paralleled the Chairman's approach to presenting the facts about identity theft patterns, generally falling into the categories of "new accounts" versus "existing accounts." However, when defining the incidence of identity Theft, the FTC continues to rely on a broader definition that includes other fraud. AFSA urges the Task Force and the FTC to utilize this report process as an opportunity to clarify the debate about identity theft, and to utilize the more accurate description that the FTC has utilized in testimony.

We recommend defining what constitutes "sensitive personal information" -- the kind of data that must be protected and for which notification must be made in the event of a data breach -- as name, address or phone number *plus* one of 3 data elements: 1) SSN; 2) Driver's License or Other State ID card; or 3) financial account numbers, *in combination with* any password, security code, etc. needed to access the account. Information that includes publicly available information, however collected – either directly or through

agents – should not be included in the Task Force's definition of "sensitive personal information."

AFSA appreciates the opportunity to comment on this matter, and we look forward to continuing to work with the President's Identity Theft Task Force. If you have any questions, or would like to discuss further, please contact Matt Gannon, Director of Federal Government Affairs, at (202) 776-7301 or mgannon@afsamail.org.

Sincerely,

Bill Himpler
Executive Vice President, Federal Government Affairs